

# On the Hardness of Entropy Minimization and Related Problems

Mladen Kovačević, Ivan Stanojević, and Vojin Šenk

Department of Electrical Engineering, Faculty of Technical Sciences,

University of Novi Sad, 21000 Novi Sad, Serbia

Emails: {kmladen, cet\_ivan, vojin\_senk}@uns.ac.rs

**Abstract**—We investigate certain optimization problems for Shannon information measures, namely, minimization of joint and conditional entropies  $H(X, Y)$ ,  $H(X|Y)$ ,  $H(Y|X)$ , and maximization of mutual information  $I(X; Y)$ , over convex regions. When restricted to the so-called transportation polytopes (sets of distributions with fixed marginals), very simple proofs of NP-hardness are obtained for these problems because in that case they are all equivalent, and their connection to the well-known SUBSET SUM and PARTITION problems is revealed. The computational intractability of the more general problems over arbitrary polytopes is then a simple consequence. Further, a simple class of polytopes is shown over which the above problems are not equivalent and their complexity differs sharply, namely, minimization of  $H(X, Y)$  and  $H(Y|X)$  is trivial, while minimization of  $H(X|Y)$  and maximization of  $I(X; Y)$  are strongly NP-hard problems. Finally, two new (pseudo)metrics on the space of discrete probability distributions are introduced, based on the so-called variation of information quantity, and NP-hardness of their computation is shown.

**Index Terms**—Entropy minimization, maximization of mutual information, NP-complete, NP-hard, subset sum, partition, number partitioning, transportation polytope, pseudometric, variation of information.

## I. INTRODUCTION

Joint entropy  $H(X, Y)$ , conditional entropies  $H(X|Y)$ ,  $H(Y|X)$ , and mutual information  $I(X; Y)$ , are some of the founding concepts of information theory. In the present paper we investigate some natural optimization problems associated with these functionals, namely, minimization of joint and conditional entropies and maximization of mutual information over convex polytopes, and show that all these problems are NP-hard. Certain special cases of these problems are found to represent information theoretic analogues of the well-known SUBSET SUM and PARTITION problems. Our results will thus provide a simple, yet interesting connection between complexity theory and information theory.

Various optimization problems for the above mentioned information measures are studied in the literature. An important example is the well-known *Maximum entropy principle* formulated by Jaynes [9], which states that, among all probability distributions satisfying certain constraints (expressing our knowledge about the system), one should pick the one with maximum entropy. It has been recognized by Jaynes, as well as many other researchers, that this choice gives the least biased, the most objective distribution consistent with the information one possesses about a system. Maximizing

entropy under constraints is therefore an important problem, and it has been thoroughly studied (see, e.g., [7], [10]).

It has also been argued [11], [15] that minimum entropy distributions can be of as much interest as maximum entropy distributions. The MinMax information measure, for example, has been introduced in [11] as a measure of the amount of information contained in a given set of constraints, and it is based both on maximum and minimum entropy distributions. More generally, entropy minimization is also very important conceptually. Watanabe [14] has shown that many algorithms for clustering and pattern recognition can be characterized as suitably defined entropy minimization problems.

Since entropy is a concave<sup>1</sup> functional, its maximization can be solved by standard concave maximization methods. On the other hand, concave minimization is in general a much harder problem [12]. Indeed, we will show that the minimization of joint entropy over convex polytopes is NP-hard. In fact, we will show that a much more restrictive problem is NP-hard, that of entropy minimization over the so-called transportation polytopes, i.e., entropy minimization under constraints on the marginal distributions. Restricting the problem to transportation polytopes is perhaps the key step in our analysis and has several advantages. First, it enables one to obtain a very simple proof of NP-hardness by using a reduction from the SUBSET SUM problem and some simple information theoretic identities and inequalities. Second, it will immediately follow from this proof that the problems of minimization of conditional entropies and maximization of mutual information are also NP-hard. This claim looks difficult to prove by some other methods because these functionals are neither concave nor convex.

Maximization of mutual information is certainly an important problem, studied in many different scenarios. A familiar example is computing the capacity of the channel which amounts to the maximization of this functional over all input distributions. This is again a convex maximization problem for which efficient algorithms exist [3]. In Section V we will show that the reverse problem – maximizing mutual information over conditional distributions, given the input distribution – is NP-hard. Another important example is the so-called *Maximum mutual information (MMI) criterion* used in the design of classifiers. See, e.g., [1], [8] for two important

<sup>1</sup> To avoid possible confusion, concave means  $\cap$  and convex means  $\cup$ .

applications of this principle.

## II. BASIC DEFINITIONS

This section reviews the definitions and basic properties of the quantities that will be used later.

### A. Shannon information measures

Shannon entropy of a random variable  $X$  with probability distribution  $P = (p_i)$  is defined as:

$$H(X) \equiv H(P) = - \sum_i p_i \log p_i \quad (1)$$

with the usual convention  $0 \log 0 = 0$  being understood. For a pair of random variables  $(X, Y)$  with joint distribution  $S = (s_{i,j})$  and marginal distributions  $P = (p_i)$  and  $Q = (q_j)$ , the following defines their joint entropy:

$$H(X, Y) \equiv H_{X,Y}(S) = - \sum_{i,j} s_{i,j} \log s_{i,j}, \quad (2)$$

conditional entropy:

$$H(X|Y) \equiv H_{X|Y}(S) = - \sum_{i,j} s_{i,j} \log \frac{s_{i,j}}{q_j}, \quad (3)$$

and mutual information:

$$I(X; Y) \equiv I_{X;Y}(S) = \sum_{i,j} s_{i,j} \log \frac{s_{i,j}}{p_i q_j}, \quad (4)$$

again with appropriate conventions. All of these quantities are related by simple identities:

$$\begin{aligned} H(X, Y) &= H(X) + H(Y) - I(X; Y) \\ &= H(X) + H(Y|X) \end{aligned} \quad (5)$$

and obey the following inequalities:

$$\max \{H(X), H(Y)\} \leq H(X, Y) \leq H(X) + H(Y), \quad (6)$$

$$\min \{H(X), H(Y)\} \geq I(X; Y) \geq 0, \quad (7)$$

$$0 \leq H(X|Y) \leq H(X). \quad (8)$$

Equalities on the right-hand sides of (6)–(8) are achieved if and only if  $X$  and  $Y$  are independent. Equalities on the left-hand sides of (6) and (7) are achieved if and only if  $X$  deterministically depends on  $Y$ , or vice versa. Another way to put this is that their joint distribution (written as a matrix) has at most one nonzero entry in every row, or in every column. Equality on the left-hand side of (8) holds if and only if  $X$  deterministically depends on  $Y$ . We will use these properties in our proofs. For their demonstration we point the reader to the standard reference [3].

From identities (5) one can make the following simple, but crucial, observation: Over a set of two-dimensional probability distributions with fixed marginals (and hence fixed marginal entropies  $H(X)$  and  $H(Y)$ ), all the above functionals differ up to an additive constant (and a minus sign in the case of mutual information). This means in particular that the minimization of joint entropy over such domains is equivalent to the minimization of either one of the conditional entropies,

or to the maximization of mutual information. Therefore, NP-hardness of any of these problems will imply that all of them are NP-hard. And finally, this will imply that more general problems of minimization/maximization of the corresponding functionals over arbitrary convex polytopes are NP-hard.

### B. Transportation polytopes

Let  $\Gamma_n^{(1)}$  and  $\Gamma_{n \times m}^{(2)}$  denote the sets of one- and two-dimensional probability distributions with alphabets of size  $n$  and  $n \times m$ , respectively:

$$\Gamma_n^{(1)} = \{(p_i) \in \mathbb{R}^n : p_i \geq 0, \sum_i p_i = 1\} \quad (9)$$

$$\Gamma_{n \times m}^{(2)} = \{(p_{i,j}) \in \mathbb{R}^{n \times m} : p_{i,j} \geq 0, \sum_{i,j} p_{i,j} = 1\} \quad (10)$$

Now consider the set of all distributions with marginals  $P \in \Gamma_n^{(1)}$  and  $Q \in \Gamma_m^{(1)}$ , denoted  $\mathcal{C}(P, Q)$ :

$$\mathcal{C}(P, Q) = \left\{ S \in \Gamma_{n \times m}^{(2)} : \sum_j s_{i,j} = p_i, \sum_i s_{i,j} = q_j \right\} \quad (11)$$

(letter  $\mathcal{C}$  stands for coupling). It is easy to show that sets  $\mathcal{C}(P, Q)$  are convex and closed in  $\Gamma_{n \times m}^{(2)}$ . They are also clearly disjoint and cover entire  $\Gamma_{n \times m}^{(2)}$ , i.e., they form a partition of  $\Gamma_{n \times m}^{(2)}$ . Finally, they are parallel affine  $(n-1)(m-1)$ -dimensional subspaces of the  $(n \cdot m - 1)$ -dimensional space  $\Gamma_{n \times m}^{(2)}$ . (We of course have in mind the restriction of the corresponding affine spaces in  $\mathbb{R}^{n \times m}$  to  $\mathbb{R}_+^{n \times m}$ .)

The set of distributions with fixed marginals is basically the set of nonnegative matrices with prescribed row and column sums (only now we require the total sum to be one, but this is inessential). Such sets are known in discrete mathematics as transportation polytopes [2]. Their name comes from the fact that they correspond to the following problem: given  $n$  supplies  $p_1, \dots, p_n$  and  $m$  demands  $q_1, \dots, q_m$  of some "goods" (total supply and total demand being equal), describe all ways of transporting the goods so that the demands are fulfilled. For example, one possible solution to the transportation problem with  $P = (1, 3, 5)$  and  $Q = (2, 4, 3)$  would be

$$\begin{pmatrix} 1 & 0 & 0 \\ 1 & 2 & 0 \\ 0 & 2 & 3 \end{pmatrix}$$

which is obtained by the so-called north-west corner rule. The set of all possible solutions constitutes a polytope  $\mathcal{C}(P, Q)$ .

In the context of the problems studied here, the following facts will be useful. A concave continuous function over any bounded convex polytope must attain its minimum over one of the vertices of the polytope. An interesting fact about transportation polytopes is that, if the marginals are integer, that is if  $p_i, q_j \in \mathbb{N}$ , then all the vertices (observed as matrices) have only integer entries. As a consequence, if the marginals are rational, that is if  $p_i, q_j \in \mathbb{Q}$ , then all the vertices have only rational entries. Furthermore, it is not hard to see that

the description length<sup>2</sup> of the vertices is polynomial in the description length of the marginals. We shall make use of these facts in the proofs of Theorems 1 and 3.

### III. ENTROPY OVER TRANSPORTATION POLYTOPES

As we noted before, we will focus here on sets of probability distributions with fixed marginals, i.e., we will consider the above mentioned optimization problems over transportation polytopes. The problems turn out to be NP-hard even under this restriction, and this is perhaps the easiest way to prove NP-hardness of their more general versions.

Let some marginal distributions  $P$  and  $Q$  be given, and observe  $\mathcal{C}(P, Q)$ . From identities (5) one sees that over  $\mathcal{C}(P, Q)$  the minimization of  $H(X, Y)$  is equivalent to the minimization of  $H(X|Y)$  and  $H(Y|X)$ , or to the maximization of  $I(X; Y)$ , so it is enough to consider only the joint entropy for example. Joint entropy  $H(X, Y)$  is well-known to be concave in the joint distribution, and so its minimization belongs to a wide class of concave minimization problems which are in general intractable [12]. Conditional entropies  $H(X|Y)$  and  $H(Y|X)$  are neither concave nor convex in the joint distribution, but over  $\mathcal{C}(P, Q)$  they are concave because in that case they differ from the joint entropy only by an additive constant. By the same reasoning, mutual information is convex in the joint distribution over  $\mathcal{C}(P, Q)$ . Based on concavity one concludes that the optimizing distribution for these problems must be one of the vertices of  $\mathcal{C}(P, Q)$ . The trouble with concave functions, of course, is that one must visit all of them, or at least a "large" portion of them, to decide where the minimum is.

#### A. The computational problems

The most general form of the problem in the context studied here would be the following: Given a polytope (by a system of inequalities, say) in  $\Gamma_{n \times m}^{(2)}$ , find the distribution (matrix)  $S$  which minimizes the entropy functional  $H_{X,Y}(S)$ . The decision version of this problem is obtained by giving some threshold  $h$  at the input, and asking whether a given polytope contains a distribution  $S$  with  $H_{X,Y}(S) \leq h$ .

Let us now restrict the problem to transportation polytopes. Since:

$$H(X, Y) \geq \max \{H(X), H(Y)\}, \quad (12)$$

over the transportation polytope  $\mathcal{C}(P, Q)$  we have:

$$H(X, Y) \geq \max \{H(P), H(Q)\} \quad (13)$$

with equality if and only if  $Y$  deterministically depends on  $X$ , or vice versa [3]. In other words, we will have equality in (13) iff the joint distribution is such that it has at most one nonzero entry in every row, or in every column. We can now formulate an even more restrictive problem, with the threshold specified in advance: Given a transportation polytope  $\mathcal{C}(P, Q) \in \Gamma_{n \times m}^{(2)}$ , is there a distribution  $S$  in this polytope with  $H_{X,Y}(S) \leq H(P)$ ? Note that, because of (13), this inequality must in fact be an equality. We name this problem ENTROPY

MINIMIZATION even though the name would probably be more appropriate for the more general problems mentioned above.

#### Problem: ENTROPY MINIMIZATION

**Instance:** Positive rational numbers  $p_1, \dots, p_n$  and  $q_1, \dots, q_m$ , with  $\sum_{i=1}^n p_i = \sum_{j=1}^m q_j = 1$ .

**Question:** Is there a matrix  $S \in \mathcal{C}(P, Q)$  with entropy  $H_{X,Y}(S) = H(P)$ ?

This problem will be shown to be NP-complete.

We also briefly note here that the corresponding problem of the maximization of  $H(X, Y)$  (maximization of  $H(X|Y)$  or minimization of  $I(X; Y)$ ) over  $\mathcal{C}(P, Q)$  is trivial because:

$$H(X, Y) \leq H(X) + H(Y) \quad (14)$$

with equality if and only if  $X$  and  $Y$  are independent [3], i.e., iff their joint distribution is  $P \times Q = (p_i q_j)$ , and this distribution clearly belongs to  $\mathcal{C}(P, Q)$ .

#### B. The proof of NP-hardness

We describe first the SUBSET SUM, a well-known NP-complete problem [6], which will be the basis of the proof to follow:

#### Problem: SUBSET SUM

**Instance:** Positive integers  $d_1, \dots, d_n$  and  $s$ .

**Question:** Is there a  $J \subseteq \{1, \dots, n\}$  such that  $\sum_{j \in J} d_j = s$ ?

*Theorem 1:* ENTROPY MINIMIZATION is NP-complete.

*Proof:* We shall demonstrate a reduction from the SUBSET SUM problem to the ENTROPY MINIMIZATION problem. Let there be given an instance of the SUBSET SUM problem, i.e., a set of positive integers  $s, d_1, \dots, d_n$ ,  $n \geq 2$ . Let  $D = \sum_{i=1}^n d_i$ , and let  $p_i = d_i/D$ ,  $q = s/D$ . The question we are trying to answer is whether there is a  $J \subseteq \{1, \dots, n\}$  such that  $\sum_{j \in J} d_j = s$ . Observe that this is equivalent to asking whether there is a matrix  $S$  with row sums  $P = (p_1, \dots, p_n)$  and column sums  $Q = (q, 1 - q)$ , which has at most one nonzero entry in every row (or, in probabilistic language, such that  $Y$  deterministically depends on  $X$ ). We know that in this case, and only in this case, the entropy of  $S$  would be equal to  $H(P)$  [3]. So if we create an instance of the ENTROPY MINIMIZATION problem with  $P$  and  $Q$  as above, the answer to the question whether there exists  $S \in \mathcal{C}(P, Q)$  with  $H_{X,Y}(S) = H(P)$  will solve the SUBSET SUM problem. Therefore, this is the reduction we wanted. It is left to prove that ENTROPY MINIMIZATION belongs to NP. This is done by using the familiar characterization of the class NP via certificates [13]. We have to show that every YES-instance of the problem has a succinct certificate, while no NO-instance has one, and that the validity of the alleged certificates can be verified in polynomial time. The certificate is of course the optimizing distribution itself. That it is succinct is easy to show (see the comment in the last paragraph of Section II-B), and polynomial time verifiability is even easier, because we only have to check that  $S$  belongs to  $\mathcal{C}(P, Q)$  and that it has at most one nonzero entry in every row. ■

<sup>2</sup> By the description length of an object, we mean the number of bits required to write it down, as usual in the context of algorithmic problems.

As a straightforward consequence of the above claim, the more general problem of finding a minimizing distribution is NP-hard. It is an interesting task to determine the precise complexity of this problem (in the sense of proving that it is complete for some natural complexity class). Note that even determining whether it belongs to FNP<sup>3</sup> is nontrivial. Whether the decision version of this problem, namely, deciding whether a given polytope contains a distribution with entropy smaller than a given threshold, belongs to NP is also an interesting question (which we shall not be able to resolve here). One has to be careful when reasoning about "certificates" for these problems. Namely, one has to be able to check in polynomial time that the certificate is indeed valid. In the above proof, we only had to check that the given matrix (the alleged certificate) belongs to  $\mathcal{C}(P, Q)$  (i.e., that it has nonnegative entries and prescribed row and column sums) and that it has at most one nonzero entry in every row, and this is clearly easy to do. But in the more general problems mentioned above, one is required to compute numbers of the form  $a \log a$  to check whether  $H(T) \leq h$  for example. These numbers are in general irrational, and therefore verifying this inequality might not be computationally trivial as it might seem. It is interesting to mention in this context the so-called Sqrt Sum problem:

**Problem:** Sqrt Sum

**Instance:** Positive integers  $d_1, \dots, d_n$ , and  $k$ .

**Question:** Decide whether  $\sum_{i=1}^n \sqrt{d_i} \leq k$ ?

This problem, though "conceptually simple" and bearing certain resemblance with checking of certificates in the general versions of the entropy minimization problem, is not known to be solvable in NP [5] (it is solvable in PSPACE).

#### IV. TWO PSEUDOMETRICS WHICH ARE HARD TO COMPUTE

A variant of the minimization of the above mentioned quantities produces a distance on the space of discrete probability distributions. For a pair of random variables  $(X, Y)$  with joint distribution  $S$ , define [4]:

$$\begin{aligned} \Delta(X, Y) &\equiv \Delta(S) = H(X, Y) - I(X; Y) \\ &= H(X|Y) + H(Y|X) \\ \Delta'(X, Y) &\equiv \Delta'(S) = 1 - \frac{I(X; Y)}{H(X, Y)} \end{aligned} \quad (15)$$

The quantity  $\Delta(X, Y)$  is sometimes called the *variation of information*. Its normalized variant,  $\Delta'(X, Y)$ , is basically an information theoretic analogue of the Jaccard distance between finite sets. Both of these quantities satisfy the properties of a pseudometric [4]. However, when this statement is made, one must assume that the joint distribution of  $(X, Y)$  is given because joint entropy and mutual information are not defined otherwise. This is usually overlooked in the literature. Furthermore, if these quantities are used as distance measures on the space of all random variables, then joint distributions of every pair of random variables must be given. For example, one

could first define some random process  $(X_t)$  and then take  $\Delta$  or  $\Delta'$  as distances between the random variables  $X_t$ . In order to avoid the dependence on the chosen random process (or on some universal joint distribution), and to define a distance between individual random variables (more precisely, between their distributions) one can make the following definitions:

$$\begin{aligned} \underline{\Delta}(P, Q) &= \inf_{S \in \mathcal{C}(P, Q)} \{H_{X,Y}(S) - I_{X,Y}(S)\}, \\ \underline{\Delta}'(P, Q) &= \inf_{S \in \mathcal{C}(P, Q)} \left\{1 - \frac{I_{X,Y}(S)}{H_{X,Y}(S)}\right\}. \end{aligned} \quad (16)$$

This definition mimics the one for the total variation distance:

$$d_V(X, Y) = \inf_{c(P, Q)} \{\mathbb{P}(X \neq Y)\} \quad (17)$$

where the infimum is taken over all joint distributions of the random vector  $(X, Y)$  with marginals  $P$  and  $Q$ .

Let  $\Gamma^{(1)} = \{(p_i)_{i \in \mathbb{N}} : p_i \geq 0, \sum_i p_i = 1\}$ . We have the following.

**Proposition 1:**  $\underline{\Delta}$  and  $\underline{\Delta}'$  are pseudometrics on  $\Gamma^{(1)}$ .

The proof of this proposition is not difficult but we omit it here since it is not essential for our current aims. We can now prove one more intractability result.

**Theorem 2:** Given rational  $P$  and  $Q$ , determining whether  $\underline{\Delta}(P, Q) = H(P) - H(Q)$  is NP-hard.

*Proof:* Note that

$$\begin{aligned} \underline{\Delta}(P, Q) &= \inf_{S \in \mathcal{C}(P, Q)} \{H_{X,Y}(S) - I_{X,Y}(S)\} \\ &= 2 \inf_{S \in \mathcal{C}(P, Q)} \{H_{X,Y}(S)\} - H(P) - H(Q). \end{aligned} \quad (18)$$

Now the claim follows directly from Theorem 1. ■

#### V. ONE MARGINAL FIXED

In this section we address similar problems as before, only now we fix only one of the marginal distributions, say  $P = (p_1, \dots, p_n)$ . If the cardinality of the alphabet of the other random variable  $Y$  is not specified, then the problems are trivial. Namely, one takes  $Q = P$  and for  $S = \text{diag}(P)$  (two-dimensional distribution with masses  $p_i$  on the diagonal and zeros elsewhere) one has  $H_{X,Y}(S) = I_{X,Y}(S) = H(P)$ , and hence  $S$  is optimal. So assume that the cardinality of the other alphabet is bounded to  $m$ . Denote the set of all distributions with marginal distribution of  $X$  fixed to  $P$  and the cardinality of the alphabet of  $Y$  fixed to  $m$ , by  $\mathcal{C}(P, m)$ . We have

$$\mathcal{C}(P, m) = \bigcup_{Q \in \Gamma_m^{(1)}} \mathcal{C}(P, Q). \quad (19)$$

Minimization of the joint entropy  $H(X, Y)$  over such polytopes is trivial. The reason is that  $H(X, Y) \geq H(P)$  with equality iff  $Y$  deterministically depends on  $X$ , and so the solution is *any* joint distribution having at most one nonzero entry in each row. Since  $H(X)$  is fixed, this also minimizes the conditional entropy  $H(Y|X)$ . The other two optimization problems considered so far, minimization of  $H(X|Y)$  and maximization of  $I(X; Y)$ , are still equivalent because  $I(X; Y) = H(X) - H(X|Y)$ , but they turn out to

<sup>3</sup> The class FNP captures the complexity of function problems associated with decision problems in NP, see [13].

be much harder. Therefore, in the following we shall consider only the maximization of  $I(X; Y)$ .

When one marginal is fixed, choosing the optimal joint distribution amounts to choosing the optimal conditional distribution  $p(y|x)$ . Mutual information  $I(X; Y)$  is known to be convex in the conditional distribution [3] (and hence,  $H(X|Y)$  is concave in  $p(y|x)$ , for fixed  $p(x)$ ) and so this is again a convex maximization problem. This conditional distribution can be thought of as a discrete memoryless communication channel with  $n$  input symbols and  $m$  output symbols, and hence we name the corresponding computational problem OPTIMAL CHANNEL.

**Problem:** OPTIMAL CHANNEL

**Instance:** Positive rational numbers  $p_1, \dots, p_n$  with  $\sum_{i=1}^n p_i = 1$ , and an integer  $m$ .

**Question:** Is there a channel  $C \in \mathcal{C}(P, m)$  with mutual information  $I_{X;Y}(C) \geq \log m$ ?

Note that the above inequality must in fact be an equality because over  $\mathcal{C}(P, m)$ :

$$I(X; Y) \leq \min \{H(P), \log m\} \quad (20)$$

which follows from (7) and the fact that  $H(Y) \leq \log m$ . The above problem is a suitable restriction of a more general problem of finding a maximizing distribution, as we did with ENTROPY MINIMIZATION.

#### A. The proof of NP-hardness

We describe next the well-known PARTITION (or NUMBER PARTITIONING) problem [6].

**Problem:** PARTITION

**Instance:** Positive integers  $d_1, \dots, d_n$ .

**Question:** Is there a partition of  $\{d_1, \dots, d_n\}$  into two subsets with equal sums?

This is clearly a special case of the SUBSET SUM problem. It can be solved in pseudo-polynomial time by dynamic programming methods [6]. But the following closely related problem is much harder.

**Problem:** 3-PARTITION

**Instance:** Nonnegative integers  $d_1, \dots, d_{3m}$  and  $k$  with  $k/4 < d_j < k/2$  and  $\sum_j d_j = mk$ .

**Question:** Is there a partition of  $\{1, \dots, 3m\}$  into  $m$  subsets  $J_1, \dots, J_m$  (disjoint and covering  $\{1, \dots, 3m\}$ ) such that  $\sum_{j \in J_i} d_j$  are all equal? (The sums are necessarily  $k$  and every  $J_i$  has 3 elements.)

This problem is NP-complete in the strong sense [6], i.e., no pseudo-polynomial time algorithm for it exists unless  $P=NP$ .

The following theorem will establish that, given an information source, determining the best channel (in the sense of having the largest mutual information) is NP-hard.

**Theorem 3:** OPTIMAL CHANNEL is NP-complete.

**Proof:** We prove the claim by reducing 3-PARTITION to OPTIMAL CHANNEL. Let there be given an instance of the

3-PARTITION problem as described above, and let  $p_i = d_i/D$  where  $D = \sum d_i$ . Deciding whether there exists a partition with described properties is clearly equivalent to deciding whether there is a matrix  $C \in \mathcal{C}(P, m)$  with the other marginal  $Q$  being uniform and  $C$  having at most one nonzero entry in every row (i.e.,  $Y$  deterministically depending on  $X$ ). This on the other hand happens if and only if there is a matrix  $C \in \mathcal{C}(P, m)$  with mutual information equal to  $H(Q) = \log m$ . Therefore, solving the OPTIMAL CHANNEL problem with instance  $(p_i)$  as above will solve the 3-PARTITION problem. This shows the NP-hardness of OPTIMAL CHANNEL. It is left to prove that it belongs to NP. The reasoning here is completely analogous to the one in the proof of Theorem 1, namely, the certificate is the optimal distribution/matrix itself. ■

The problem remains NP-complete even over  $\mathcal{C}(P, 2)$ , i.e., when the cardinality of the channel output is fixed in advance to 2. In that case the problem is equivalent to the PARTITION problem.

It is easy to see that the transformation in the proof of Theorem 3 is in fact *pseudo-polynomial* [6] which implies that OPTIMAL CHANNEL is strongly NP-complete and, unless  $P=NP$ , has no pseudo-polynomial time algorithm.

#### ACKNOWLEDGMENT

The authors would like to acknowledge the financial support of the Ministry of Science and Technological Development of the Republic of Serbia (grants No. TR32040 and III44003).

#### REFERENCES

- [1] R. Battiti, "Using Mutual Information for Selecting Features in Supervised Neural Net Learning", *IEEE Transactions on Neural Networks*, vol. 5, pp. 537–550, 1994.
- [2] R. A. Brualdi, *Combinatorial Matrix Classes*, Cambridge University Press, 2006.
- [3] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Second edition, Wiley-Interscience, John Wiley and Sons, Inc., 2006.
- [4] I. Csiszár and J. Körner, *Information Theory: Coding Theorems for Discrete Memoryless Systems*, Academic Press, Inc., 1981.
- [5] K. Etessami and M. Yannakakis, "On the Complexity of Nash Equilibria and Other Fixed Points", *SIAM Journal on Computing*, vol. 39 (6), pp. 2531–2597, 2010.
- [6] M. R. Garey and D. S. Johnson, *Computers and Intractability: A Guide to the Theory of NP-completeness*, A Series of Books in the Mathematical Sciences, W. H. Freeman and Co., 1979.
- [7] P. Harremoës and F. Topsøe, "Maximum Entropy Fundamentals", *Entropy*, vol. 3, pp. 191–226, Sept. 2001.
- [8] X. He, L. Deng, and W. Chou, "Discriminative Learning in Sequential Pattern Recognition", *IEEE Signal Processing Magazine*, vol. 25, pp. 14–36, 2008.
- [9] E. T. Jaynes, "Information Theory and Statistical Mechanics", *Physical Reviews*, vol. 106, pp. 620–630, vol. 108, pp. 171–190, 1957.
- [10] J. N. Kapur, *Maximum-Entropy Models in Science and Engineering*, New Delhi, India: Wiley, 1989.
- [11] J. N. Kapur, G. Baciú, and H. K. Kesavan, "The MinMax Information Measure", *Int. J. Systems Sci.*, vol. 26, pp. 1–12, 1995.
- [12] S. Onn, *Nonlinear Discrete Optimization: An Algorithmic Theory*, European Mathematical Society, 2010.
- [13] C. H. Papadimitriou, *Computational Complexity*, Addison-Wesley Publishing Company, Reading, MA, 1994.
- [14] S. Watanabe, "Pattern Recognition as a Quest for Minimum Entropy", *Pattern Recognition*, vol. 13, pp. 381–387, 1981.
- [15] L. Yuan and H. K. Kesavan, "Minimum Entropy and Information Measure", *IEEE Transactions on Systems, Man and Cybernetics - Part C*, vol. 28, pp. 488–491, 1998.